

## Encryption key application technique for use with electronic integrated circuits

**Patent number:** FR2738970

**Publication date:** 1997-03-21

**Inventor:** RHELIMI ALAIN; ROSE RENE

**Applicant:** SCHLUMBERGER IND SA (FR)

**Classification:**

**- international:** **G06K19/067; G07F7/10; H01L23/58; H04L9/22;**  
**G06K19/067; G07F7/10; H01L23/58; H04L9/18; (IPC1-**  
**7); H04L9/10; G06F12/14; G06K19/073**

**- european:** **G06K19/067; G07F7/10D4E; G07F7/10D12;**  
**H01L23/58B; H04L9/22**

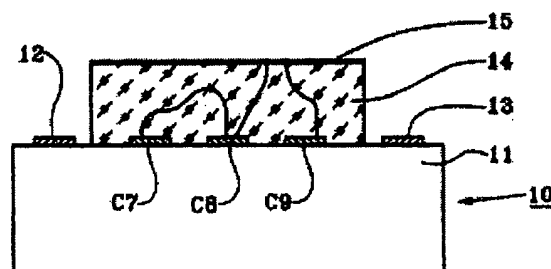
**Application number:** FR19950011078 19950919

**Priority number(s):** FR19950011078 19950919

**Report a data error here**

### Abstract of FR2738970

The method for determining the encryption key associated with an integrated circuit (10) having a memory plane (11) comprises a first step of forming a matrix of N electrical contacts on the surface of the memory plane (11). The second step includes depositing a layer (14) of a material having random in-homogeneous electrical resistivity on the matrix. The next step including the determination of the encryption key or resistive key (Kr) on the basis of the random distribution of electrical resistances connecting the various electrical contacts (Ci) of the matrix.



Data supplied from the esp@cenet database - Worldwide

10/2/05  
(19) RÉPUBLIQUE FRANÇAISE  
INSTITUT NATIONAL  
DE LA PROPRIÉTÉ INDUSTRIELLE  
PARIS

(11) N° de publication :  
(à n'utiliser que pour les  
commandes de reproduction)

2 738 970

(21) N° d'enregistrement national : 95 11078

(51) Int Cl<sup>8</sup> : H 04 L 9/10, G 06 K 19/073, G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION

A1

(22) Date de dépôt : 19.09.95.

(30) Priorité :

(43) Date de la mise à disposition du public de la  
demande : 21.03.97 Bulletin 97/12.

(56) Liste des documents cités dans le rapport de  
recherche préliminaire : *Se reporter à la fin du  
présent fascicule.*

(60) Références à d'autres documents nationaux  
apparentés :

(71) Demandeur(s) : SCHLUMBERGER INDUSTRIES SA  
SOCIÉTÉ ANONYME — FR.

(72) Inventeur(s) : RHEIMI ALAIN et ROSE RENE.

(73) Titulaire(s) :

(74) Mandataire : SCHLUMBERGER INDUSTRIES.

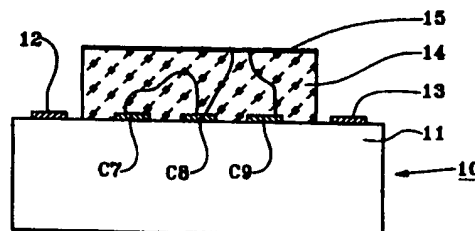
(54) PROCÉDE DE DETERMINATION D'UNE CLE DIVERSIFIEE ASSOCIEE A UN CIRCUIT INTEGRE.

(57) Procédé de détermination d'une clé diversifiée asso-  
ciée à un circuit intégré (10) présentant un plan-mémoire  
(11).

Selon l'invention, le procédé comporte les étapes suivan-  
tes:

- (a) réaliser une matrice de N contacts électriques  $C_i$  ( $i = 1, \dots, N$ ) à la surface dudit plan-mémoire (11),
- (b) déposer sur ladite matrice une couche (14) d'un ma-  
tériau à résistivité électrique inhomogène aléatoire,
- (c) déterminer ladite clé diversifiée à partir de la réparti-  
tion aléatoire des résistances électriques reliant les diffé-  
rents contacts électriques  $C_i$  de la matrice.

Application à la sécurisation des cartes à mémoire utili-  
sées en télévision cryptée.



FR 2 738 970 - A1



**PROCEDE DE DETERMINATION D'UNE CLE DIVERSIFIEE  
ASSOCIEE A UN CIRCUIT INTEGRE**

5 La présente invention concerne un procédé de détermination d'une clé diversifiée associée à un circuit intégré. Elle concerne également un circuit intégré sécurisé mettant en oeuvre ledit procédé.

10 L'invention trouve une application particulièrement avantageuse dans le domaine de la sécurisation des cartes à mémoire, notamment les cartes à mémoire utilisées en télévision cryptée.

15 D'une manière générale, les cartes à mémoire comportent un corps de carte en matériau plastique et un module électronique inséré dans une cavité aménagée dans ledit corps de carte. Le module électronique est constitué d'un circuit intégré, ou puce, placé sur un support lui-même muni de plages métalliques destinées à assurer la liaison électrique entre le module et un lecteur de cartes. Le circuit intégré peut être une mémoire du type EEPROM, pour l'application aux télécartes par exemple, ou un microprocesseur, pour les applications aux cartes bancaires, à la téléphonie mobile ou encore à la télévision cryptée.

20 La plupart des cartes à mémoire sont donc utilisées pour effectuer des transactions électroniques, ce qui naturellement ne manque de susciter la tentation de frauder les systèmes mettant en oeuvre des cartes à mémoire de manière à pouvoir bénéficier sans contrepartie financière des services fournis par ces systèmes.

25 Afin d'éviter, ou du moins de limiter la fraude, les informations échangées avec le module électronique des cartes à mémoire sont cryptées selon des procédés variés qui font l'objet d'une abondante littérature. Il suffit seulement de savoir que les messages reçus par les circuits intégrés des cartes sont chiffrés à l'aide de clés, dites clés diversifiées, stockées dans le plan-mémoire des circuits. Ces clés peuvent elles-mêmes être protégées d'une lecture extérieure en masquant le niveau du plan-mémoire dans lequel elles sont  
30 inscrites par plusieurs niveaux de métal faisant office d'écran tout en participant à la dynamique du circuit.

Toutefois, le degré de sécurisation obtenu n'est pas absolu car il est toujours possible pour un fraudeur expérimenté d'accéder aux clés secrètes par une analyse fonctionnelle du circuit intégré.

5 Aussi, le problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de détermination d'une clé diversifiée associée à un circuit intégré présentant un plan-mémoire, procédé qui permettrait d'atteindre un niveau de protection des clés diversifiées beaucoup plus élevé du fait  
10 notamment d'un stockage statique des clés hors du plan-mémoire et donc inaccessible par analyse fonctionnelle du circuit.

La solution au problème technique posé consiste, selon la présente invention, en ce que ledit procédé comporte les étapes suivantes :

- 15 (a) réaliser une matrice de N contacts électriques  $C_i$  ( $i = 1, \dots, N$ ) à la surface dudit plan-mémoire,
- (b) déposer sur ladite matrice une couche d'un matériau à résistivité électrique inhomogène aléatoire,
- (c) déterminer ladite clé diversifiée à partir de la répartition  
20 aléatoire des résistances électriques reliant les différents contacts électriques  $C_i$  de la matrice.

Ainsi, on utilise la structure résistivement aléatoire de ladite couche comme générateur de la clé diversifiée associée au circuit intégré. Celle-ci n'est donc jamais stockée dans le plan-mémoire du circuit et, de ce fait, est reconstruite à chaque mise sous tension  
25 du circuit intégré. De plus, on peut observer que la couche de matériau réalise un écran qui protège le circuit contre toutes lectures frauduleuses. Si cette couche est enlevée ou altérée, la clé est modifiée et les informations demeureront cryptées à jamais. Il est impossible de lire par un moyen extérieur au circuit intégré les  
30 valeurs des résistances prises en compte par le procédé de l'invention pour déterminer la clé diversifiée.

Afin d'améliorer encore le degré de sécurisation conféré par le procédé conforme à l'invention, il est prévu qu'il comporte à la suite de l'étape (b) une étape consistant à disposer un écran

métallique sur ladite couche de matériau à résistivité électronique inhomogène aléatoire.

Selon un mode de mise en oeuvre particulier du procédé selon l'invention, on réalise ledit matériau à résistivité électrique  
5 inhomogène aléatoire en mélangeant une encre à faible résistivité électrique à une encre à forte résistivité électrique.

Enfin, un circuit intégré sécurisé présentant un plan-mémoire est remarquable, selon la présente invention, en ce qu'il comporte une matrice de N contacts électriques  $C_i$  ( $i=1, \dots, N$ ) à la surface  
10 dudit plan-mémoire, une couche d'un matériau à résistivité électrique inhomogène aléatoire, déposée sur ladite matrice, et des moyens de détermination de ladite clé diversifiée à partir de la répartition aléatoire des résistances électriques reliant les différents contacts électriques  $C_i$  de la matrice.

15 La description qui va suivre en regard des dessins annexés, donnés à titre d'exemples non limitatifs, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est une vue de côté d'un circuit intégré sécurisé par la mise en oeuvre du procédé selon l'invention.

20 La figure 2 est une vue de dessus du circuit intégré de la figure 1.

La figure 3 est un schéma de moyens de détermination d'une clé diversifiée associée au circuit intégré des figures 1 et 2.

25 La figure 4 est le schéma équivalent des moyens de détermination de la figure 3.

Le circuit intégré 10 montré aux figures 1 et 2 présente un plan-mémoire 11, ou face active, sur lequel sont formés des plots métalliques d'entrée/sortie, tels que 12 et 13 sur les figures 1 et 2, destinés à être reliés par des fils conducteurs aux plages  
30 métalliques d'un support, non représenté, qui constitue avec le circuit intégré 10 le module électronique d'une carte à mémoire.

Comme on peut le voir sur les figures 1 et 2, une matrice de N, ici 9, contacts électriques  $C_i$  ( $i = 1, \dots, 9$ ) a été réalisée à la surface du plan-mémoire 11 du circuit 10. Cette matrice de  
35 contacts électriques est recouverte, par sérigraphie par exemple,

d'une couche 14 d'un matériau à résistivité électrique inhomogène aléatoire, tel qu'un mélange d'une encre à faible résistivité électrique avec une encre à forte résistivité électrique. La couche 14 de matériau a, par exemple, une épaisseur de l'ordre de 10  $\mu\text{m}$  au plus.

Ainsi que le montrent les figures 1 et 2, les chemins de courant entre les différents contacts électriques  $C_i$  de la matrice peuvent prendre des formes très variées résultant de la structure aléatoire de la résistivité électrique à l'intérieur de la couche 14. C'est cette répartition aléatoire des résistances électriques entre les contacts  $C_i$  qui constitue la base du procédé de détermination d'une clé diversifiée associée au circuit intégré 10, ladite clé étant en quelque sorte une expression numérisée de la répartition des résistances, comme cela sera expliqué en détail plus loin.

Notons que la clé secrète du circuit étant finalement contenue dans la couche 14 de matériau, il y a avantage à protéger ladite couche en la recouvrant d'un écran métallique 15 qui peut d'ailleurs participer lui-même à l'établissement des chemins de courant comme l'indique la figure 2.

De même que la couche 14, l'écran métallique 15 peut avoir une épaisseur de 10  $\mu\text{m}$  (à cet égard le dessin de la figure 2 n'est pas à l'échelle).

On a représenté sur la figure 3 un schéma des moyens utilisés pour la détermination de la clé diversifiée appliquée à la structure de circuit des figures 1 et 2.

Ces moyens de détermination comportent un bus comprenant une ligne  $L_1$  à une première tension  $V_{CC}$ , une ligne  $L_2$  de mesure et une ligne  $L_3$  à une deuxième tension  $V_{SS}$ . Chaque ligne  $L_1$ ,  $L_2$ ,  $L_3$  du bus peut être reliée à un contact électrique de la matrice par l'intermédiaire de trois interrupteurs analogiques commandables  $K_1$ ,  $K_2$ ,  $K_3$  respectivement. En d'autres termes, chaque contact  $C_i$  peut être connecté à une et une seule des lignes  $L_1$ ,  $L_2$ ,  $L_3$  du bus.

Le circuit intégré 10 commande les interrupteurs analogiques  $K_1$ ,  $K_2$ ,  $K_3$  de manière à définir un ensemble de triplets de contacts électriques noté  $(C_j, C_i, C_k)_l$ , au nombre de  $M$  ( $l = 1, \dots$ ,

M), les contacts  $C_j$ ,  $C_i$  et  $C_k$  étant respectivement reliés aux lignes  $L_1$ ,  $L_2$ ,  $L_3$  du bus. On obtient alors le circuit équivalent de la figure 4 dans laquelle  $R_{ij}$  et  $R_{ik}$  représentent les résistances électriques reliant le contact  $C_i$  aux contacts  $C_j$  et  $C_k$  respectivement.

- 5 De manière à pouvoir effectuer une comparaison significative des résistances  $R_{ij}$  et  $R_{ik}$ , il y a avantage à ce que, pour chaque triplet  $(C_j, C_i, C_k)_l$ , les contacts  $C_j$  et  $C_k$  soient équidistants du contact  $C_i$ . Dans ce cas, les résistances  $R_{ij}$  et  $R_{ik}$ , bien qu'équivalentes, sont en général différentes du fait de  
10 l'inhomogénéité aléatoire de la résistivité électrique de la couche 14 de matériau. On utilise alors cette différence pour affecter à chaque triplet  $(C_j, C_i, C_k)_l$  un bit  $b_l$  défini par convention par :

$$b_l = 1 \quad \text{si } R_{ij} > R_{ik}$$

$$b_l = 0 \quad \text{si } R_{ij} < R_{ik}$$

- 15 On a ainsi un ensemble aléatoire de  $M$  bits  $b_l$  qui, rangés selon une suite ordonnée, détermine la clé diversifiée à attribuer au circuit intégré 10.

En pratique, la tension de la ligne  $L_2$  de mesure est comparée à  $(V_{CC} + V_{SS})/2$ , le signe de cette comparaison permettant d'établir  
20 l'information logique  $b_l$ . Cette technique de mesure de résistance relative a l'avantage de s'affranchir des variations de température et de tension.

Il faut également noter que les résistances additionnelles de mesure doivent être très faibles pour ne pas diminuer l'influence de  
25 la dispersion des résistances non homogènes à mesurer. En effet, les canaux de mesure ont eux-même des dispersions qui, si elles devenaient trop importantes, rendraient insuffisantes l'influence et la modification de la couche 14 de matériau, ce qui ouvrirait une possibilité de fraude.

- 30 Dans l'exemple de la matrice  $3 \times 3$  des figures 1 et 2, les triplets satisfaisant la condition d'équidistance sont :

$(C_1, C_2, C_3)_1$ ,  $(C_4, C_5, C_6)_2$ ,  $(C_7, C_8, C_9)_3$

$(C_4, C_1, C_2)_4$ ,  $(C_2, C_3, C_6)_5$ ,  $(C_8, C_9, C_6)_6$ ,  $(C_4, C_7, C_8)_7$

$(C_1, C_4, C_7)_8$ ,  $(C_2, C_5, C_8)_9$ ,  $(C_3, C_6, C_9)_{10}$

35  $(C_1, C_5, C_9)_{11}$ ,  $(C_7, C_5, C_3)_{12}$ ,

$(C_1, C_7, C_9)_{13}, (C_1, C_3, C_9)_{14},$   
 $(C_2, C_7, C_9)_{15}, (C_1, C_8, C_3)_{16},$   
 $(C_2, C_4, C_8)_{17}, (C_2, C_6, C_8)_{18}$

5        On obtient alors 18 bits  $b_i$  associés chacun à un des 18 triplets, d'où une clé diversifiée à 18 bits.

          Au besoin, la clé obtenue peut être corrigée par un code correcteur d'erreur stocké en mémoire à la personnalisation de la carte. Toutefois, ce code ne permet pas de retrouver la clé si on ne dispose pas de la clé initiale.

10



## REVENDICATIONS

1. Procédé de détermination d'une clé diversifiée associée à un circuit intégré (10) présentant un plan-mémoire (11),  
 5 caractérisé en ce que ledit procédé comporte les étapes suivantes :
  - (a) réaliser une matrice de N contacts électriques  $C_i$  ( $i = 1, \dots, N$ ) à la surface dudit plan-mémoire (11),
  - (b) déposer sur ladite matrice une couche (14) d'un matériau  
 10 à résistivité électrique inhomogène aléatoire,
  - (c) déterminer ladite clé diversifiée à partir de la répartition aléatoire des résistances électriques reliant les différents contacts électriques  $C_i$  de la matrice.
2. Procédé selon la revendication 1, caractérisé en ce que l'étape  
 15 (c) de détermination de ladite clé diversifiée consiste à :
  - définir un ensemble de M triplets  $(C_j, C_i, C_k)_l$  ( $l = 1, \dots, M$ ) de contacts électriques,
  - affecter à chaque triplet un bit  $b_l$  défini par convention par :  
 20
 
$$b_l = 1 \quad \text{si } R_{ij} > R_{ik}$$

$$b_l = 0 \quad \text{si } R_{ij} < R_{ik}$$
 $R_{ij}$  et  $R_{ik}$  étant les résistances électriques reliant le contact  $C_i$  aux contacts  $C_j$  et  $C_k$  respectivement,
  - construire la clé diversifiée sous la forme d'une suite  
 25 ordonnée des M bits  $b_l$ .
3. Procédé selon la revendication 2, caractérisé en ce que pour chaque triplet  $(C_j, C_i, C_k)_l$  les contacts  $C_j$  et  $C_k$  sont équidistants du contact  $C_i$ .
4. Procédé selon l'une quelconque des revendications 1 à 3,  
 30 caractérisé en ce qu'il comporte à la suite de l'étape (b) une étape consistant à déposer un écran métallique (15) sur ladite couche (14) de matériau à résistivité électrique inhomogène aléatoire.
5. Procédé selon l'une quelconque des revendications 1 à 4,  
 35 caractérisé en ce qu'on réalise ledit matériau à résistivité

électrique inhomogène aléatoire en mélangeant une encre à faible résistivité électrique à une encre à forte résistivité électrique.

- 5 6. Circuit intégré sécurisé présentant un plan-mémoire (11), caractérisé en ce qu'il comporte une matrice de N contacts électriques  $C_i$  ( $i = 1, \dots, N$ ) à la surface dudit plan-mémoire (11), une couche (14) d'un matériau à résistivité électrique inhomogène aléatoire, déposée sur ladite matrice, et des
  - 10 moyens de détermination de ladite clé diversifiée à partir de la répartition aléatoire des résistances électriques reliant les différents contacts électriques  $C_i$  de la matrice.
7. Circuit intégré sécurisé selon la revendication 6, caractérisé en ce que lesdits moyens de détermination de ladite clé diversifiée sont aptes à :
  - 15 - définir un ensemble de M triplets  $(C_j, C_i, C_k)_l$  ( $l = 1, \dots, M$ ) de contacts électriques,
  - affecter à chaque triplet un bit  $b_l$  défini par convention par :
 
$$b_l = 1 \quad \text{si } R_{ij} > R_{ik}$$

$$b_l = 0 \quad \text{si } R_{ij} < R_{ik}$$
 20  $R_{ij}$  et  $R_{ik}$  étant les résistances électriques reliant le contact  $C_i$  aux contacts  $C_j$  et  $C_k$  respectivement,
  - construire la clé diversifiée sous la forme d'une suite ordonnée des M bits  $b_l$ .
- 25 8. Circuit intégré sécurisé selon la revendication 7, caractérisé en ce que pour chaque triplet  $(C_j, C_i, C_k)_l$  les contacts  $C_j$  et  $C_k$  sont équidistants du contact  $C_i$ .
9. Circuit intégré sécurisé selon l'une des revendications 7 ou 8, caractérisé en ce que lesdits moyens de détermination de la
  - 30 clé diversifiée comportent, d'une part, un bus comprenant une ligne ( $L_1$ ) à une première tension  $V_{CC}$ , une ligne ( $L_2$ ) de mesure et une ligne ( $L_3$ ) à une deuxième tension  $V_{SS}$ , d'autre part, et trois interrupteurs analogiques commandables ( $K_1, K_2, K_3$ ) destinés à relier chaque contact  $C_i$  à l'une des lignes ( $L_1, L_2, L_3$ ).
  - 35

10. Circuit intégré sécurisé selon l'une quelconque des revendications 6 à 9, caractérisé en ce que ladite couche (14) de matériau à résistivité électrique inhomogène aléatoire est recouverte d'un écran métallique (15).
- 5 11. Circuit intégré sécurisé selon l'une quelconque des revendications 6 à 10, caractérisé en ce que ledit matériau à résistivité électrique inhomogène aléatoire est un mélange d'une encre à forte résistivité électrique et d'une encre à faible résistivité électrique.

1/2

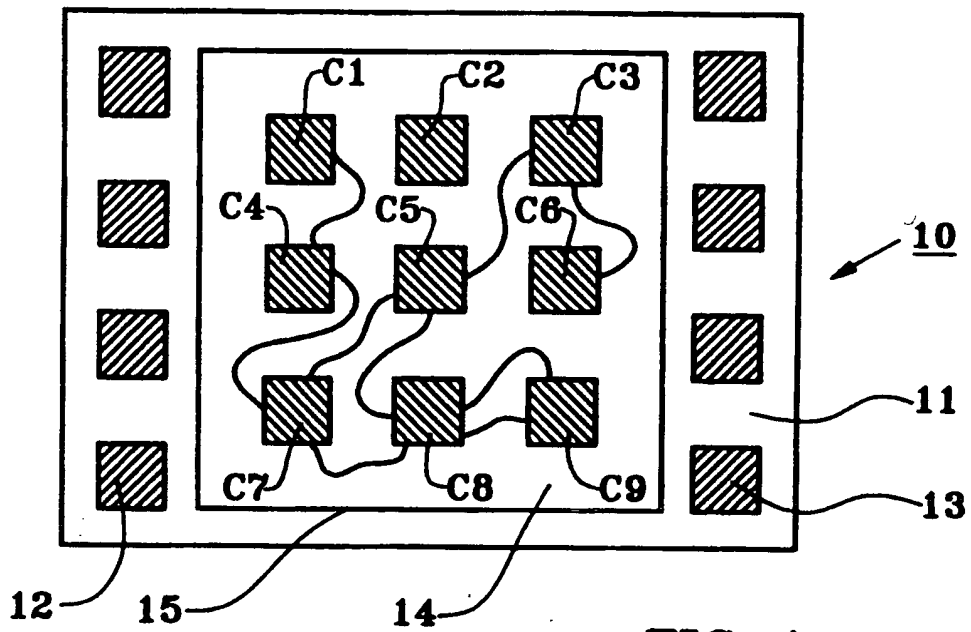


FIG. 1

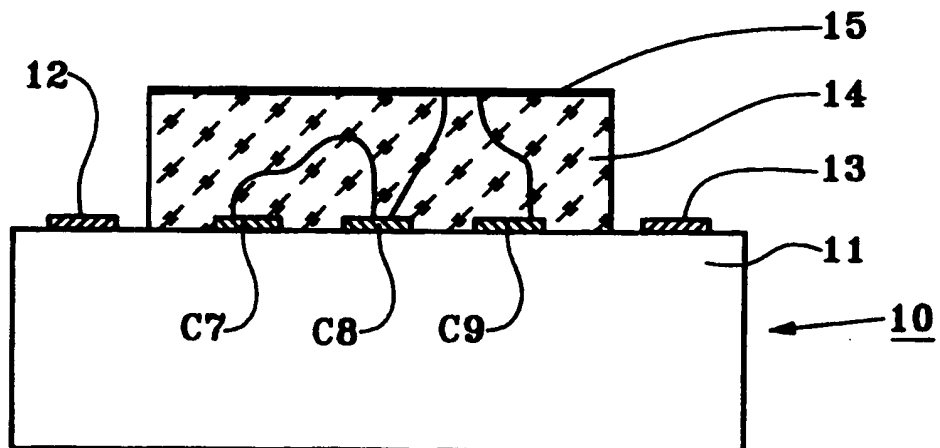


FIG. 2

2/2

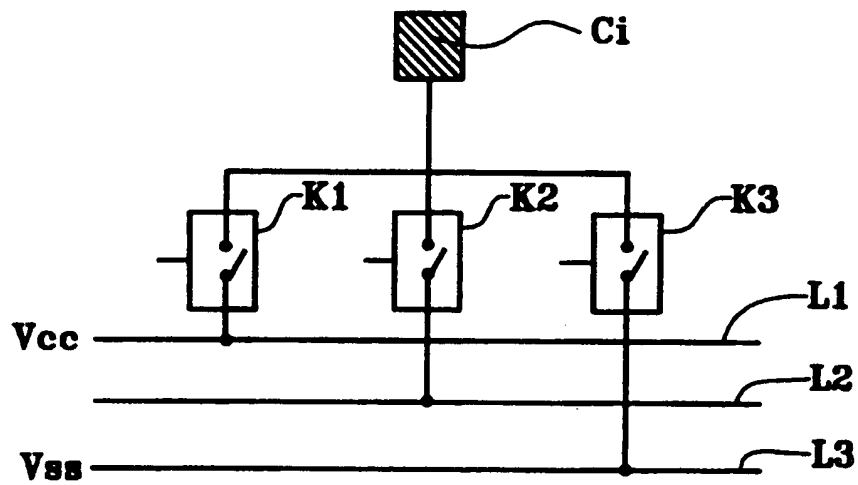


FIG. 3

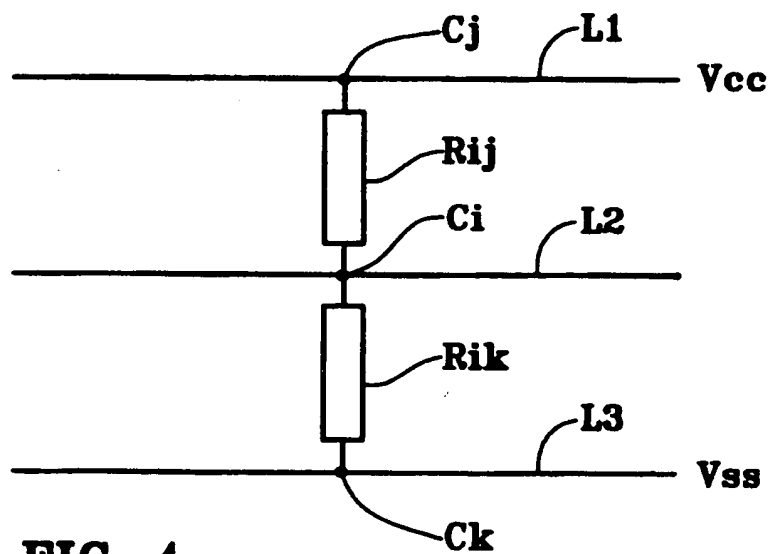


FIG. 4

INSTITUT NATIONAL  
de la  
PROPRIETE INDUSTRIELLE

**RAPPORT DE RECHERCHE  
PRELIMINAIRE**  
établi sur la base des dernières revendications  
déposées avant le commencement de la recherche

FA 519591  
FR 9511078

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande actuelle
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	EP-A-0 583 709 (THOMSON CONSUMER ELECTRONICS) * le document en entier *	1,6
A	US-A-4 591 189 (R.E. HOLMEN) * abrégé; figure 5 * * colonne 4, ligne 10 - ligne 30 *	1,4,6,10
A	FR-A-2 471 083 (ELECTRONIQUE MARCEL DASSAULT)	
A	DE-A-42 43 888 (GAO)	
A	US-A-3 636 318 (G. LINDSTROM)	
		DOMAINES TECHNIQUES RECHERCHES (Art. CL. 9)
		G07F G06K
Date d'achèvement de la recherche		Examinateur
5 Juillet 1996		David, J
<p><b>CATEGORIE DES DOCUMENTS CITES</b></p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : pertinent à l'encontre d'un ou de plusieurs revendications ou artifice-plus technologique général O : divulgation non écrite P : document intermédiaire</p> <p>T : théorie en principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons A : membre de la même famille, document correspondant</p>		